

Remarks

Claims 24-25 are amended through this Amendment and Response. Claims 1-8, 10-12 and 14-31 are pending in this application. Each of the pending claims is believed to define an invention that is novel and unobvious over the cited references. Based on the foregoing amendment and the following remarks, it is respectfully submitted that the instant application is in condition for allowance. Prompt reconsideration and withdrawal of the rejections is earnestly requested.

Rejection under 35 U.S.C. § 112, Second Paragraph

Claims 24 and 25 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Action objects to the term “substantially” as rendering the claim indefinite. The Applicant respectfully traverses. However, to expedite the prosecution of this application, claims 24 and 25 have been amended to overcome this rejection. Reconsideration of the claims and allowance thereof is respectfully requested.

Rejection under 35 U.S.C. § 103 over Davies and Arnold

Claims 1-8 and 15-18 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Davies et al., *Security for Computer Networks*, p. 140-168 (“Davies”), in view of U.S. Patent No. 6,175,924 to Arnold (“Arnold”). This rejection is respectfully traversed.

To establish a *prima facie* case for obviousness under 35 U.S.C. § 103(a), three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, ***the prior art reference (or references when combined) must teach or suggest all the claim limitations.*** See M.P.E.P. § 2143 (emphasis added). It is submitted that the combination of the above-mentioned references fails to teach each and every element of the claimed invention for at least the reasons provided below. Thus, it is respectfully submitted that the combination fails to establish a *prima facie* case for obviousness under 35 U.S.C. § 103(a).

Claim 1 recites a “method for transferring a first root key between a key provider system and a second other system via an information network.” The method comprises, among other features, “providing within the second other system a **first secure module having a second super-root key within a read-only memory circuit thereof** and provided with the first secure module, the second super-root key accessible only by program code being executed on a processor internal to the first secure module, and wherein the second super-root key is other than modifiable and other than accessible outside of the module” (emphasis added). It is submitted that this feature is neither taught nor suggested by the combination of Davies and Arnold.

In rejecting claim 1, the Action concedes that Davies does not teach the use of a secure module having a super-root key within a read-only memory circuit thereof. The Action asserts, however, that Arnold teaches such a secure module, aligning the claimed secure module with Arnold’s teachings of a security card 11 as shown in FIG. 1 of Arnold. Applicant respectfully disagrees.

Arnold teaches a method and system for verifying the authenticity of an application program. The system of Arnold includes a main processor 15 for executing the application program. In one embodiment, the system of Arnold also includes a security card 11, also referred to as a cryptographic adapter 11, coupled to a RAM 53 and a ROM 55. *See Arnold, Col. 3: 48-56.* The RAM 53 and ROM 55 of Arnold are used for storing “the program’s executable instructions,” and not for storing encryption keys of any sort, including private keys, root keys, or super root keys. *Id.* Thus, Arnold does not teach the recited “first secure module having a second super-root key within a read-only memory circuit thereof.” Accordingly, it is respectfully submitted that the combination of Davies and Arnold fails to teach each and every element of claim 1.

Moreover, even if, *arguendo*, the recited “first secure module” was sufficiently taught by Arnold, such teachings could not be combined by the teachings of Davies. On pages 158-167, Davies describes the international standard ISO 8732 entitled *Banking – Key Management (Wholesale)*, covering key management procedures for safeguarding the secret cryptographic keys used to protect banking messages. *See Davies, p. 158, first paragraph.* Davies does not elaborate on how the KK and the DK are distributed. However, Davies does state that under the standard, “keying material which set up the basic keys on which the key hierarchy depends” is distributed manually. *Davies, p. 158, sixth paragraph (emphasis added).* In a three-layer key hierarchy described in pages 159-160 of Davies, the KKM is the basic key on which the rest of the hierarchy depends. Thus, in the three-layer key hierarchy disclosed by Davies, the KKM is distributed manually to the banks. Since the KKM is distributed manually, it cannot be stored in a read-only memory circuit. Accordingly, Davies essentially teaches away from using a secure module having a read-only memory circuit. If Arnold’s alleged teachings of a secure module were implemented

into the key system of Davies, such system would be inoperable, because the banks would be unable to store the manually-distributed KKM into the secured module. Accordingly, it is respectfully submitted that the cited references could not have been combined in order to render claim 1 obvious under 35 U.S.C. § 103(a).

In addition to the above-mentioned features, claim 1 further recites “executing program code on the processor internal to the first secure module to decrypt the encrypted first root key using the second super-root key stored within the read-only memory circuit of the first secure module and to store the decrypted first root key internally within a secure key memory location of the first secure module, wherein the first root key is useable for at least one of encrypting or decrypting private keys, and **wherein a bit length of the first super-root key is greater than a bit length of the first root key, and said bit length of the first root key is greater than a bit length of any of said private keys** being encrypted or decrypted” (emphasis added). It is submitted that this feature is not taught or suggested by the combination of Davies and Arnold.

In rejecting claim 1, the Action appears to align the aforementioned limitations with Davies’ teachings of double-length keys on pages 160-161. Specifically, Davies teaches using double length keys for key encryption keys (i.e., KK or KKM), where two single length keys of 64-bit size each are concatenated to form a double length key. Although Davies teaches using double-length keys at the higher levels of the hierarchy, it only teaches using two key lengths. Thus, although Davies teaches using a single-length key for a DK (i.e. private key) and using a double-length key for a KK (i.e. root key), there is no teaching or suggestion in Davies that a KKM (i.e. super root key) can have a greater key length than the KK while the KK has a greater key length than the DK. In other words, since Davies teaches only a single and a double key length, there is no way for a

KKM key length to be greater than a KK key length while the KK key length is also greater than the DK key length. In Davies, at least two of the DK, the KK, and the KKM must have the same key length. Thus, Davies does not teach “a bit length of the first super-root key is greater than a bit length of the first root key, and said bit length of the first root key is greater than a bit length of any of said private keys being encrypted or decrypted,” as recited in claim 1.

Arnold does not cure the deficiencies of Davies in teaching the aforementioned features. Specifically, Arnold does not include any teachings of a key-encryption-key, root key, and super root key, nor does it include any teachings of bit lengths related to the keys. Accordingly, it is respectfully submitted that Davies and Arnold, individually or in combination, fail to teach or suggest each and every element of claim 1. Withdrawal of the rejection of claim 1 and allowance thereof is respectfully requested.

Claim 15 includes features similar to claim 1 and is submitted as allowable for at least the same reasons. Claims 2-8 and 16-18 are dependent on claims 1 and 15, respectfully, and are submitted as allowable for at least the same reasons.

Rejection under 35 U.S.C. § 103 over Davies, Arnold, and Spelman

Claims 10-12 and 14 are rejected under 35 U.S.C. § 103(a) as being unpatentable over the modified Davies and Arnold and in further view of Patent No. 5,680,458 to Spelman et. al (“Spelman”). These rejections are respectfully traversed.

Claim 10 recites features similar to claim 1. Therefore, for at least the same reasons previously discussed, claim 10 is patentably distinguishable over the combination of Davies and

Arnold. Spelman fails to cure the deficiencies of Davies and Arnold previously discussed. Specifically, Spelman is relied on by the Action for its alleged teachings of second and third encryption keys. Spelman does not teach or suggest a secure module having a read-only memory or key length relating to encryption keys. Accordingly, it is respectfully submitted that claim 10 is patentably distinguishable over the prior art and should be allowed. Claims 11-12 and 14 are dependent on claim 10 and should be allowed for at least the same reasons. Withdrawal of the rejections and reconsideration of claims 10-12 and 14 is respectfully requested.

Rejection under 35 U.S.C. § 103 over Davies, Arnold, Spelman, and Mason

Claims 21-24 and 31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over the modified Davies, Arnold, Spelman, and in further view of U.S. Patent No. 6,331,784 to Mason et. al ("Mason"). These rejections are respectfully traversed.

Claim 21 recites features similar to claim 1. Therefore, for at least the same reasons previously discussed, claim 21 is patentably distinguishable over the combination of Davies, Arnold, and Spelman. Mason fails to cure the deficiencies of Davies, Arnold, and Spelman previously discussed. Specifically, Mason is relied on by the Action for its alleged teachings of a system with an erase only mode. Mason does not teach or suggest a secure module having a read-only memory or key length relating to encryption keys. Accordingly, it is respectfully submitted that claim 21 is patentably distinguishable over the prior art and should be allowed. Claims 22-24 and 31 are dependent on claim 21 and should be allowed for at least the same reasons. Withdrawal of the rejections and reconsideration of claims 21-24 and 31 is respectfully requested.

Rejection under 35 U.S.C. § 103 over Davies, Arnold, and Easter

Claims 19 and 26 are rejected under 35 U.S.C. § 103(a) as being unpatentable over the modified Davies and Arnold and in further view of Patent No. 5,598,889 to Easter (“Easter”). These rejections are respectfully traversed.

Claims 19 and 26 are respectively dependent on claims 15 and 21. Therefore, for at least the same reasons previously discussed, claims 19 and 26 are patentably distinguishable over the combination of Davies and Arnold. Easter fails to cure the deficiencies of Davies and Arnold previously discussed. Specifically, Easter is relied on by the Action for its alleged teachings of a FIPS 140 compliant module. Easter does not teach or suggest a secure module having a read-only memory or key length relating to encryption keys. Accordingly, it is respectfully submitted that claims 19 and 26 are patentably distinguishable over the prior art and should be allowed. Withdrawal of the rejections and reconsideration of claims 19 and 26 is respectfully requested.

Rejection under 35 U.S.C. § 103 over Davies, Arnold, Easter, and Bergum

Claims 20 and 27 are rejected under 35 U.S.C. § 103(a) as being unpatentable over the modified Davies, Arnold, and Easter, and in further view of U.S. Patent No. 5,249,277 to Bergum et. al (“Bergum”). Applicant respectfully traverses this rejection.

Claims 20 and 27 are respectfully dependent on claims 15 and 21. Therefore, for at least the same reasons previously discussed, claims 20 and 27 are patentably distinguishable over Davies in combination with Arnold and Easter. Bergum fails to cure the deficiencies of Davies, Arnold, and Easter previously discussed. Specifically, Bergum is relied on by the Action for its alleged

teachings of a tamper detection circuit. Bergum does not teach or suggest a secure module having a read-only memory or key length relating to encryption keys. Accordingly, it is respectfully submitted that claims 20 and 27 is patentably distinguishable over the prior art and should be allowed. Withdrawal of the rejections and reconsideration of claims 20 and 27 is respectfully requested.

Rejection under 35 U.S.C. § 103 over Davies, Arnold, Spelman, Mason, and Ehram

Claim 25 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Davies, Arnold, Spelman, and Mason, and in further view of U.S. Patent No. 4,386,234 to Ehram et. al (“Ehram”). Applicant respectfully traverses this rejection.

Claim 25 is indirectly dependent on claim 21. Therefore, for at least the same reasons previously discussed for claim 21, claim 25 is patentably distinguishable over Davies, Arnold, Spelman, and Mason. Ehram fails to cure the deficiencies of Davies, Arnold, Spelman, and Mason previously discussed. Specifically, Ehram is relied on by the Action for its alleged teachings of a non-volatile reprogrammable memory. Ehram does not teach or suggest a secure module having a read-only memory or key length relating to encryption keys. Accordingly, it is respectfully submitted that claim 25 is patentably distinguishable over the prior art and should be allowed. Withdrawal of the rejections and reconsideration of claim 25 is respectfully requested.

Rejection under 35 U.S.C. § 103 over Davies, Arnold, Spelman, Mason, and Ober

Claims 28-31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over the modified Davies, Arnold, Spelman, and Mason, and in further view of U.S. Patent No.6,307,936 to Ober et al. (“Ober”). Applicant respectfully traverses this rejection.

Claims 28-31 are dependent on claims 1, 10, 15, and 21, respectfully. Therefore, for at least the same reasons previously discussed for claim 28-31 are patentably distinguishable over the modified Davies, Arnold, Spelman, and Mason. Ober fails to cure the deficiencies of Davies, Arnold, Spelman, and Mason previously discussed. Specifically, Ober is relied on by the Action for its alleged teachings of exact ranges of key length. Ehram does not teach or suggest a secure module having a read-only memory, nor does it teach “a bit length of the first super-root key is greater than a bit length of the first root key, and said bit length of the first root key is greater than a bit length of any of said private keys being encrypted or decrypted,” as recited in claim 1. Accordingly, it is respectfully submitted that claims 28-31 are patentably distinguishable over the prior art and should be allowed. Withdrawal of the rejections and reconsideration of claim 28-31 is respectfully requested.

Conclusion

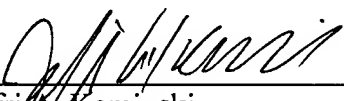
All of the stated grounds of rejection have been properly traversed. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is hereby invited to telephone the undersigned at the number provided.

No additional fees are believed to be required. However, if the Office deems that any fees are necessary, authorization is hereby granted to charge any required fees to Deposit Account No. 22-0261.

In view of the above amendment, applicant believes the pending application is in condition for allowance. Prompt and favorable consideration of this Amendment is respectfully requested.

Dated: 7/13/07

Respectfully submitted,

By 
Jeffrey A. Kaminski
Registration No.: 42,709
James R. Burdett
Registration No.: 31,594
VENABLE LLP
P.O. Box 34385
Washington, DC 20043-9998
(202) 344-4000
(202) 344-8300 (Fax)
Attorney/Agent For Applicant